Docket No.: GB920010007US1 (7161-224U) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Customer Number: 46320
Paul ABBOT	:	Confirmation Number: 9940
Application No.: 10/046,058	:	Group Art Unit: 2134
Filed: January 10, 2002	:	Examiner: T. Szymanski

For: METHOD AND APPARATUS FOR STORAGE OF SECURITY KEYS AND CERTIFICATES

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed September 7, 2006, in response to the Examiner reopening prosecution in the Office Action dated March 2, 2007, wherein Appellant appeals from the Examiner's rejection of claims 1-34.

I. REAL PARTY IN INTEREST

This application is assigned to IBM Corporation by assignment recorded on January 10, 2002, at Reel 012503, Frame 0914.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1-34 are pending and four-times rejected in this Application. It is from the multiple rejections of claims 1-34 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

The claims have not been amended subsequent to the imposition of the Fourth Office Action dated March 2, 2007 (hereinafter the Fourth Office Action).

V. SUMMARY OF CLAIMED SUBJECT MATTER

Referring to Figures 1 and 2 and to independent claims 1 and 23, a method for storage of security keys and certificates in a data processing system is disclosed. In step 210, at least one entity (150) is provided in the form of a key or certificate for storage in a storage means (page 14, lines 18-21). In steps 240 and 250, the entity is fragmented into fragments (152, 154) of non-uniform length according to a predetermined algorithm (200) (page 14, lines 25-26). In step 260, the fragments (152, 154) are stored in the storage means (280) (page 14, line 27). In steps 270 and 280, the fragments (152, 154) of the at least one entity (150) are intermixed within the storage means (page 14, lines 27-30). Referring to claim 3, the storage means also contains random bit patterns (120) (page 10, lines 1-7). Referring to claim 5, the location of storing the fragments (152, 154) is also determined by the algorithm (200) (page 11, lines 3-5).

Referring to Figure 1 and to independent claim 13, an apparatus for storage of security keys and certificates in a data processing system is disclosed. The apparatus includes a storage means (page 7, lines 19-24), at least one entity (150) in the form of a key or certificate for storage in the storage means (page 12, lines 8-16), and the entity (150) is stored in fragments

(152, 154) of non-uniform length according to a predetermined algorithm (200) and fragments of the at least one entity (150) are intermixed within the storage means (page 14, lines 16-18).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-2, 4-9, 11-14, 16-24, 26-31, and 33-34 were rejected under 35 U.S.C. § 103 for obviousness based upon Kausik, U.S. Patent Publication No. 2001/0008012, in view of Bahls et al., U.S. Patent No. 5,706,513 (hereinafter Bahls);

2. Claims 10 and 32 were rejected under 35 U.S.C. § 103 for obviousness based upon Kausik in view of Bahls; and

3. Claims 3, 15, and 25 were rejected under 35 U.S.C. § 103 for obviousness based upon Kausik in view of Bahls and further in view of Henson et al., U.S. Patent No. 7,003,109 (hereinafter Henson).

VII. ARGUMENT

THE REJECTION OF CLAIMS 1-2, 4-9, 11-14, 16-24, 26-31, AND 33-34 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON KAUSIK IN VIEW OF BAHLS

For convenience of the Honorable Board in addressing the rejections, claims 16 and 27 stand or fall together with claim 5, and claims 2, 4, 6-9, 11-14, 17-24, 26, 28-31, and 33-34 stand or fall together with independent claim 1.

Claims 1, 13, and 23

Independent claims 1, 13, and 23 each recite an entity "in the form of a key or certificate" and that the entity is fragmented into fragments of non-uniform length. Appellant notes that in the Third Office Action dated June 7, 2006, the Examiner rejected claims 1-6, 9, 11-17, 20-28,

and 31-34 for anticipation based upon Bahls. In an Appeal Brief dated November 7, 2006 (hereinafter First Appeal Brief), Appellant present several arguments as to why Bahls fails to identically disclose the claimed invention within the meaning of 35 U.S.C. 102. Among Appellant's arguments, Appellant argued that Bahls fails to teach (i) an entity, in the form of a key, is fragmented and (ii) the entity is fragmented into fragments of non-uniform length.

On page 2 of the Fourth Office Action, the Examiner introduced the present rejection and asserted the following:

> Kausik teaches storage of security keys and certificates in a storage means, but fails to explicitly teach fragmenting the keys or certificates. (Kausik Figure 1, paragraphs 11, 24-32).

Thus, the Examiner appears to be arguing that Kausik teaches that the entity is the form of a key. The Examiner then relies upon Bahls to teach the remaining of the limitations. In so doing the Examiner asserted the following on pages 2 and 3 of the Fourth Office Action:

> However, in related art, Bahls discloses a system for the storage and fragmentation of files. (Bahls et al Col 5 lines 55-67 - Col 6 lines 1-3, figure 6).
>
> As taught by Kausik (paragraph 27) the keys/certificates are stored in any standard storage medium including floppy disks, hard disks, magnetic stripe cards, and smart cards, such media as taught by Bahls is advantageously shared amongst several applications. Wherein the working storage of a given application is not large enough to store an entire data object it is desirable to fragment such a data object into multiple pieces and store those pieces (Bahls Col 1 lines 55-67, Col 2 lines 2-20, Col 3 lines 35-40). Additionally, such fragments when for instance N=2 exists for a given object (key or certificate) and the size is not a multiple of the segment size will be of a non-uniform nature in length when stored and intermixed in the storage medium (Bahls Col 5 lines 55-67).

The Examiner's asserted rationale for modifying Kausik in view of Bahls is found in the second full paragraph on page 3 of the Fourth Office Action and reproduced below:

> It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Bahls with those of Kausik in order to facilitate shared storage amongst applications wherein the working storage of those given applications is not adequate to store an entire working object.

Appellant respectfully submits that one having ordinary skill in the art would not have been motivated to modify Kausik in view of Bahls in the manner suggested by the Examiner.

The stated rationale by Bahls for fragmenting a data object Obj 1 is that "if the data object Obj 1 is larger than the available storage capacity of the working storage 112" (column 5, lines 35-37). Moreover, Bahls states that it is not necessary to fragment the data object Obj 1 "if the data object Obj 1 is smaller than the available storage capacity of the working storage 112" (column 5, lines 27-39). However, claim 1 recites that the "fragments (152, 154) of the at least one entity (150) are intermixed within the storage means." If the scenario (i.e., size of fragments less than available storage capacity of storage means) implied by the limitations are applied to the teachings of Bahls, then one having ordinary skill in the art would recognize that Bahls would teach, in this scenario, that the data object Obj 1 (i.e., corresponding to the claimed entity in the form of a key or certificate) would not be fragmented. Thus, based upon the teachings of Bahls, one having ordinary skill in the art would not have arrived at the claimed invention based upon the teachings of Bahls.

Moreover, Appellant notes that the Examiner has failed to establish any reasonable basis for explaining why one having ordinary skill in the art would look to fragment entities in the form of a key. As a general matter, keys or certificates are some of the smallest-sized entities that are typically stored. At the time of the invention, circa 2001-2002, 128 bit (equivalent, in size, to 16 bytes) encryption was considered to be extremely robust. Circa 2001-2002, hard drives were as large as 40 gigabytes (and even as large as 100 gigabytes). A gigabyte is one trillion bytes. As such, Appellant respectfully submits that one having ordinary skill in the art at the time of the invention would not consider keys or certificates to be a type of data entity that would require segmentation in order to fit into storage.

The previously-held notion that keys are so small as to not require segmentation is also supported by the teachings of Bahls. In this regard, reference is made to column 6, lines 42-54, which is reproduced below:

> In the example of FIG. 1, the data object Obj 1 does contain another segment, segment Seg 3, that must be stored on the staging queue 108. Thus, control flows to step 314, where segment Seg 3 is selected. The selected segment Seg 3 is optionally processed in step 316, and then stored on the staging queue 108 along with the private key A in step 318. This is shown in FIG. 5, where the selected segment Seg 3 and the private key A have been stored in new record 502 of the staging queue 108. After segment Seg 3 has been stored on the staging queue 108, the first application 110 determines in step 320 that the data object Obj 1 contains no other segments that must be stored on the staging queue 108. Accordingly, control moves to step 322.

As taught by Bahls, the "private key A," which is specifically generated for object Obj 1 (see column 6, lines 6-9), is stored with each of the fragments of object Obj 1 (i.e., Seg 1, Seg, 2, Seg. 3). As evident from these teachings, the private key A is small enough that including it in with each fragment makes very little difference to the overall size of the fragment and whether or not that fragment could fit into a particular working storage. Thus, for the reasons stated above, Appellant respectfully submits that one having ordinary skill in the art would not have arrived at the claimed invention based upon the teachings of Kausik and Bahls.

Claims 5, 16, and 27

Claims 5, 16, and 27 each recite that "the location of storing the fragments (152, 154) is also determined by the algorithm (200)" (emphasis added). By using the term "the," these claims refer back to the first instance of the term "algorithm." Thus, the algorithm recited in claims 5, 16, and 27 that determines the location of storing the fragments is also the same algorithm that determines how the entity is to be fragmented into fragments.

In the Third Office Action, the Examiner asserted that "[a]ny implementation that resolves such an issue must then logically be composed of an algorithm," apparently intending to assert that since the segments of the object are stored, the determination of where these segments are to be stored are a result of an algorithm. This analysis, however, fails to account for the claimed limitation that the algorithm for determining the location where the fragments are to be stored is also the same algorithm that determines how the entity is to be fragmented into fragments. The algorithm (see column 5, line 59) disclosed by Bahls does not appear to determine where the fragments are stored.

In the first full paragraph on page 10 of the Third Office Action, the Examiner responded to Appellant's arguments as follows:

> The applicant has stated "Bahls does not appear to determine where the fragments are stored", but from the disclosure of Bahls it is clear that this is exactly what the system is doing. In Bahls the data is segmented depending on the storage location since the purpose as disclosed is that the data within Bahls is too large for a single block it is segmented between several blocks thus being stored by the algorithm that segments the data object and further related to each other through the key so that the fragments may be pieced back together properly between data blocks.

The Examiner has twisted Appellant's argument. Appellant did not state that " Bahls does not appear to determine where the fragments are stored." Instead, Appellant stated that "[t]he algorithm (see column 5, line 59) disclosed by Bahls does not appear to determine where the fragments are stored "(emphasis added). Unlike the Examiner's other arguments, in which the Examiner takes a narrow claim limitation and improperly broadens the claim limitation, in this instance, the Examiner takes a very narrow argument by Appellant about what an algorithm is capable of doing and somehow broadens this argument such that Appellant is purportedly arguing that Bahls does not disclose a particular capability. As such, the Examiner has failed to directly address Appellant's argument.

Appellant presented the above arguments in the First Appeal Brief regarding the teachings of Bahls. Upon reviewing page 4 of the Fourth Office Action with regard to claim 5, Appellant notes that the Examiner has presented similar arguments as to claim 5 to those arguments that the Examiner presented in the Third Office Action. The Examiner, however, has not addressed the arguments Appellant presented in the First Appeal Brief as to claim 5. Appellant, therefore, respectfully submits that the imposed rejection of claim 5 under 35 U.S.C. § 103 for obviousness based upon Kausik in view of Bahls is not viable.

THE REJECTION OF CLAIMS 10 AND 32 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON KAUSIK IN VIEW OF BAHLS

For convenience of the Honorable Board in addressing the rejections, claim 32 stands or falls together with claim 10.

The Examiner concluded that it is well known in the art that "when a collision occurs the object is stored immediately following the occupied spot." Notwithstanding what was known or not know by one having ordinary skill in the art, the Examiner has failed to establish a prima facie case of obviousness. The Examiner has employed an "obvious to try" argument (i.e., it would have been obvious to modify Bahls since the limitation was known in the art), which is not proper. Rather, a burden is imposed upon the Examiner to identify a source in the applied prior art for each claim limitations and identify a source for the requisite realistic rationale to modify a particular reference in a particular manner to arrive at a specifically claimed invention. The Examiner, however, has failed to meet this burden.

The Examiner's Response

In the first full paragraph on page 10 of the Third Office Action, the Examiner responded to Appellant's arguments as follows:

> In support of the rejection against claim 10 the article hash collision has been provided, which details "when multiple lookup keys are mapped to identical indices... hash collision occurs. The most popular ways of dealing with this are... open addressing (searching other array indices nearby for an empty space)."

The Examiner's comments notwithstanding, the Examiner has failed to set forth the requisite factual support for the rationale to combine Kausik and Bahls so as to arrive at the claimed invention.

Appellant presented the above arguments in the First Appeal Brief regarding the teachings of Bahls. Upon reviewing page 6 of the Fourth Office Action with regard to claim 10, Appellant notes that the Examiner has presented similar arguments as to claim 10 to those arguments that the Examiner presented in the Third Office Action. The Examiner, however, has not addressed the arguments Appellant presented in the First Appeal Brief. Appellant, therefore, respectfully submits that the imposed rejection of claim 10 under 35 U.S.C. § 103 for obviousness based upon Kausik in view of Bahls is not viable.

THE REJECTION OF CLAIMS 3, 15, AND 25 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON KAUSIK IN VIEW OF BAHLS AND HENSON

For convenience of the Honorable Board in addressing the rejections, claims 3, 15, and 25 stand or fall together with independent claim 1.

Claims 3, 15, and 25 respectively depend ultimately from independent claims 1, 13, and 23, and Appellant incorporates herein the arguments previously advanced in traversing the imposed rejection of claims 1, 13, and 23 under 35 U.S.C. § 103 for obviousness based upon Kausik and Bahls. The tertiary reference to Henson does not cure the argued deficiencies of the combination of Kausik and Bahls. Accordingly, the proposed combination of references would not yield the claimed invention. Appellant, therefore, respectfully submits that the imposed rejection of claims 3, 15, and 25 under 35 U.S.C. § 103 for obviousness based upon Kausik in view of Bahls and Henson is not viable.

Conclusion

Based upon the foregoing, Appellant respectfully submits that the Examiner's rejections under 35 U.S.C. § 103 based upon the applied prior art is not viable. Appellant, therefore, respectfully solicits the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 103.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 09-0461, and please credit any excess fees to such deposit account.

Date: June 1, 2007

Respectfully submitted,

/Scott D. Paul/

Scott D. Paul
Registration No. 42,984
Steven M. Greenberg
Registration No. 44,725
Phone: (561) 922-3845
CUSTOMER NUMBER 46320

VIII. CLAIMS APPENDIX

1. A method for storage of security keys and certificates in a data processing system comprising:

providing at least one entity (150) in the form of a key or certificate for storage in a storage means;

fragmenting the entity into fragments (152, 154) of non-uniform length according to a predetermined algorithm (200);

storing the fragments (152, 154) in the storage means (280);

wherein fragments (152, 154) of the at least one entity (150) are intermixed within the storage means.

2. A method for storage as claimed in claim 1, wherein the storage means is a data file including a block of data (110) accommodating the entities (150).

3. A method for storage as claimed in claim 1, wherein the storage means also contains random bit patterns (120).

4. A method for storage as claimed in claim 1, wherein the step of fragmenting the entity (150), fragments the bytes of the entity (150).

5. A method for storage as claimed in claim 1, wherein the location of storing the fragments (152, 154) is also determined by the algorithm (200).

6. A method for storage as claimed in claim 1, wherein the entity (150) can be read from the storage means by using the algorithm (200) to find and recombine the fragments (152, 154) of the entity (150).

7. A method for storage as claimed in claim 1, wherein the storage means has a pass code (140) and the algorithm (200) for fragmenting uses the pass code (140).

8. A method for storage as claimed in claim 7, wherein the fragments (152, 154) are stored at locations in the storage means determined by using the pass code (140).

9. A method for storage as claimed in claim 1, wherein the method includes keeping a bit map (130) as a record of fragment locations until the storage is complete (190).

10. A method for storage as claimed in claim 1, wherein in the event that a fragment (152) has already been stored at a location required for a subsequent fragment (154), the subsequent fragment (154) is stored immediately after the existing fragment (152).

11. A method for storage as claimed in claim 1, wherein the storage means is a keystore repository.

12. A method for storage as claimed in claim 11, wherein the algorithm (200) is implemented as a keystore class.

13. An apparatus for storage of security keys and certificates in a data processing system comprising:

a storage means;

at least one entity (150) in the form of a key or certificate for storage in the storage means;

wherein the entity (150) is stored in fragments (152, 154) of non-uniform length according to a predetermined algorithm (200) and fragments of the at least one entity (150) are intermixed within the storage means.

14. An apparatus for storage as claimed in claim 13, wherein the storage means is a data file including a block of data (110) accommodating the entities (150).

15. An apparatus for storage as claimed in claim 13, wherein the storage means also contains random bit patterns (120).

16. An apparatus for storage as claimed in claim 13, wherein the location of the fragments (152, 154) is also determined by the algorithm (200).

17. An apparatus for storage as claimed in claim 13, wherein the entity (150) can be read from the storage means by using the algorithm (200) to find and recombine the fragments (152, 154) of the entity (150).

18. An apparatus for storage as claimed in claim 13, wherein the storage means has a pass code (140) and the algorithm (200) for fragmenting uses the pass code (140).

19. An apparatus for storage as claimed in claim 18, wherein the fragments (152, 154) are stored at locations in the storage means determined by using the pass code (140).

20. An apparatus for storage as claimed in claim 13, wherein a bit map (130) is kept as a record of fragment locations until the storage is complete (190).

21. An apparatus for storage as claimed in claim 13, wherein the storage means is a keystore repository.

22. An apparatus for storage as claimed in claim 21, wherein the algorithm (200) is implemented as a keystore class.

23. A computer program product for storage of security keys and certificates in a data processing system, said product comprising program instructions in machine-readable form on a medium, said instructions causing the system to perform the steps of:

providing at least one entity (150) in the form of a key or certificate for storage in a storage means;

fragmenting the entity into fragments (152, 154) of non-uniform length according to a predetermined algorithm (200);

storing the fragments (152, 154) in the storage means (280);

wherein fragments (152, 154) of the at least one entity (150) are intermixed within the storage means.

24. A computer program product for storage as claimed in claim 23, wherein the storage means is a data file including a block of data (110) accommodating the entities (150).

25. A computer program product for storage as claimed in claim 23, wherein the storage means also contains random bit patterns (120).

26. A computer program product for storage as claimed in claim 23, wherein the step of fragmenting the entity (150), fragments the bytes of the entity (150).

27. A computer program product for storage as claimed in claim 23, wherein the location of storing the fragments (152, 154) is also determined by the algorithm (200).

28. A computer program product for storage as claimed in claim 23, wherein the entity (150) can be read from the storage means by using the algorithm (200) to find and recombine the fragments (152, 154) of the entity (150).

29. A computer program product for storage as claimed in claim 23, wherein the storage means has a pass code (140) and the algorithm (200) for fragmenting uses the pass code (140).

30. A computer program product for storage as claimed in claim 29, wherein the fragments (152, 154) are stored at locations in the storage means determined by using the pass code (140).

31. A computer program product for storage as claimed in claim 23, wherein the instructions further cause the system to keep a bit map (130) as a record of fragment locations until the storage is complete (190).

32. A computer program product for storage as claimed in claim 23, wherein in the event that a fragment (152) has already been stored at a location required for a subsequent fragment (154), the subsequent fragment (154) is stored immediately after the existing fragment (152).

33. A computer program product for storage as claimed in claim 23, wherein the storage means is a keystore repository.

34. A computer program product for storage as claimed in claim 33, wherein the algorithm (200) is implemented as a keystore class.

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.